Michael Kind
Mk@kindlaw.com
KIND LAW FIRM
8860 S. Maryland Pkwy, Suite 106
Las Vegas, NV 89123
Tel: (702) 337-2322
Fax: (702) 329-5881

Gayle M. Blatt *(pro hac vice)*
gmb@cglaw.com
CASEY GERRY SCHENK
FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Tel: (619) 238-1811
Fax: (619) 544-9232

Attorneys for Plaintiff and the Putative Class
[Additional Counsel Listed on Signature Page]

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

RONALD STALLONE, on behalf of himself and all other persons similarly situated,

Plaintiff,

v.

FARMERS GROUP, INC., a Nevada Corporation; FARMERS INSURANCE EXCHANGE; and 21st CENTURY INSURANCE COMPANY,

Defendants.

Case No. 2:21-cv-01659-GMN-VCF

PLAINTIFF'S REPLY IN SUPPORT OF SECOND MOTION FOR LEAVE TO FILE SUPPLEMENTAL AUTHORITY CONCERNING THE MOTION TO DISMISS PLAINTIFF'S AMENDED CLASS ACTION COMPLAINT [ECF NO. 21]

Pursuant to Local Rule 7-2(g), Plaintiff Ronald Stallone, individually and on behalf of the putative class he seeks to represent, filed this Motion to alert the Court to a recent order addressing both standing and the substantive issues raised in Defendants' February 8, 2022 Motion to Dismiss Plaintiff's Amended Class Action Complaint (the "Motion to Dismiss") (ECF No. 21). That order, *In re: USAA Data Security Litigation*, Case No. 21-cv-5813 (VB), 2022 2022 WL 3348527 (S.D.N.Y. Aug. 12, 2022) (the "*USAA* Order"), provides persuasive and helpful guidance to this Court, and thus good cause exists to consider the *USAA* Order. *Accord Hunt v. Washoe Cnty. Sch. Dist.*, 2019 WL 4262510, at *3 (D. Nev. Sept. 9, 2019). Indeed, rather than address whether this Court should consider the *USAA* Order, Defendants' opposition simply reiterates the arguments already made in its motion to dismiss. And while these arguments are inappropriate here, Plaintiff will nevertheless address them below.

I. THE *USAA* ORDER PROVIDES HELPFUL GUIDANCE ON ARTICLE III STANDING QUESTIONS

Plaintiff's complaint alleges in detail multiple ways in which he has been harmed by the Unauthorized Data Disclosure ("UDD"). *See* ECF No. 49 at 1-3; Compl. ¶¶ 2-4, 7, 19-21, 23, 25, 32-34, 51-72, 87, 109.[1] And, as all parties, agree, the UDD that gave rise to this case was part of a concerted and businesslike campaign by malicious cybercriminals to steal Class Members' driver's license numbers. Under binding Ninth Circuit precedent, "data breaches in which hackers targeted PII create[] a risk of injury sufficient to support standing." *Zappos.com, Inc. v. Stevens*, 888 F.3d 1020, 1026 n.6 (9th Cir. 2018) (quoting *Atlas v. Carefirst, Inc.*, 865 F.3d 620, 629 (D.C. Cir. 2017)). Nevertheless, Defendants argue that the *USAA* Order, which applies this well-held principle to find standing for Plaintiffs in a very similar data disclosure

[1] All references to the Complaint are to the Amended Class Action Complaint, filed January 7, 2022. ECF No. 16.

to the one alleged here, is somehow inconsistent with binding Ninth Circuit precedent.[2] Defendants are wrong.

First, driver's license numbers – standing alone – are sufficiently sensitive information that their theft, in combination with other the other information compromised here (including names and addresses), creates a sufficient increased risk of harm to confer Article III standing. This is predicated on the rationale of *Zappos*, as well as *Krottner v. Starbucks Corp.*, 625 F.3d 1139 (9th Cir. 2010), where the Ninth Circuit set forth the factors where a substantial risk of identity theft confers Article III standing.

As the Ninth Circuit held in *Zappos*, the most important factor that courts consider is whether the hackers targeted PII in an effort to harm consumers. 888 F.3d at 1026 n.6. Here, Plaintiff pleads that hackers systematically pursued these driver's license numbers from the array of insurers who made this very sensitive PI available through their online quoting platforms. "Why else would hackers . . . steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Id.* (quoting *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015)). Even where no named plaintiff has yet suffered *any* identity theft, "[t]he sensitivity of the personal information, combined with its theft [meant] that the plaintiffs had adequately alleged an injury in fact supporting standing." *Id.* at 1027.

Fundamentally, Defendant's argument is that a driver's license is not a social security number and that social security numbers are somehow magic. This conclusion is belied by the

---

[2] Oddly, Defendants assert that the case law they cite is "binding" despite lacking a single citation to any Ninth Circuit case in their briefing. District court decisions, from within or without the Ninth Circuit, while persuasive, are not binding authority on this Court. *See United States v. Stott*, No. 310CR00026LRHWGC, 2020 WL 1929841, at *3 (D. Nev. Apr. 20, 2020). To the extent this Court concludes that the district court decisions cited by Defendants are inconsistent with binding Ninth Circuit precedent, it is bound to follow the higher court's guidance. *Norsoph v. Riverside Resort & Casino, Inc.*, No. 213CV00580APGEJY, 2020 WL 641223, at *11 (D. Nev. Feb. 11, 2020), *amended*, 2020 WL 8571839 (D. Nev. May 21, 2020).

holdings of both *Zappos* and *Krottner* that the proper analysis examines whether a plaintiff alleges facts supporting that the breached data *can be used to commit identity theft*, not whether the Plaintiff can invoke some special identifier. In fact, *Zappos* directly contradicts that notion by holding that even where "there is no allegation in [a] case that the stolen information included social security numbers," there is still injury-in-fact where the stolen data "gave hackers the means to commit fraud or identity theft . . . ." 888 F.3d at 1027. For example, the Ninth Circuit held "the type of information accessed in the Zappos breach [names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information] can be used to commit identity theft, including by placing them at higher risk of 'phishing' and 'pharming,' which are ways for hackers to exploit information they already have to get even more PII." *Id.* at 1023, 1027.

And here, unlike in *Zappos*, we *know* the hackers are *actually engaged* in "pharming," because it is undisputed that they "already had" personal information on Plaintiff and used it to "pharm" Farmers' online quoting platform to gain access to his driver's license number. Compl. ¶ 19. Thus, one of the very types of identity theft *Zappos* found sufficient to support injury-in-fact *already exists in this case* – no inferences needed.

Second, Plaintiff also goes further than many of the cases cited by Defendants. Here, the Complaint does not rely on bare allegations that the driver's license number is an important and sensitive piece of data that can be used in identity theft and fraud. Instead, Plaintiff cites multiple experts who explain both that an individual's driver's license number is valuable and sensitive, and explain how it is used in various types of prevalent identity theft. *Id.* ¶ 35 (quoting Tim Sadler, CEO of email security firm Tessian: "[B]ad actors may be using these driver's license numbers to fraudulently apply for unemployment benefits in someone else's name, a scam proving especially lucrative for hackers as unemployment numbers continue to soar"); ¶ 34 (quoting Experian blogger Sue Poremba regarding how the driver's license number is used to connect hackers to the DMV, employers, doctor's offices, government agencies and other entities: "*Next to your Social Security number, your driver's license is one*

of the most important pieces to keep safe from thieves.") (emphasis added); ¶ 33 (quoting Forbes writer Lee Mathews describing how driver's license numbers are valuable as a critical part of a fraudulent, synthetic identity); ¶ 37 (explaining how such valuable PI can be used to gain access to the victim's digital life, including bank accounts, social media, credit card, and tax details).

These detailed allegations distinguish Plaintiff's Complaint from those in cases cited by Defendants, in which other (nonbinding) district court decisions indicate only a failure of plaintiffs' pleadings. *Cf. In re Uber Techs., Inc., Data Sec. Breach*, No. ML 18-2826 PSG (GJSx), 2019 WL 6522843, at *4 (C.D. Cal. Aug. 19, 2019) (*Uber*); *Antman v. Uber Techs., Inc.*, No. 3:15-cv-01175-LB, 2015 WL 6123054, at *10-11 (N.D. Cal. Oct. 19, 2015) (*Antman I*). Here, where Plaintiff Stallone has explained in detail and by reference to knowledge disseminated by industry experts about the many types of identity theft which the breach of a driver's license number can cause, *Uber* and *Antman I* are inapposite. And the fact that hackers stole Plaintiff's driver's license number in a concerted campaign to collect this specific data further bolsters his contention that the breach places him at substantial risk of identity theft. *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1034 (N.D. Cal. 2019) ("Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints.") (quoting *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x. 384, 388 (6th Cir. 2016)).

In fact, Farmers admitted that identify theft is a real risk in the wake of disclosure of driver's license numbers. Farmers even offered identity theft protection and encouraged Plaintiff to use it, advising him that in addition to enrolling in Credit Monitoring, he should "order your free credit report, place a fraud alert on your credit bureau file, place a security freeze on your credit file and report suspicious activity." Compl. ¶ 25. Thus, Plaintiff's allegations make clear that a third party can very easily engage in future identity theft by using the PI that was targeted during the UDD, and are sufficient to show an immediate risk of future identity theft and harm.

Further, the Second Circuit test for standing applied in the *USAA* Order is actually more stringent than that applied by the Ninth Circuit in *Zappos* and *Krottner*, and yet the court concluded the plaintiffs there had standing. *See* Ex. 1 at 3 (citing *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 303 (2d Cir. 2021) (holding the three part test is: "(1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.")). In considering whether that was the case where (a) driver's license numbers, names, and addresses had been exposed, (b) to hackers who *already had possession* of some information about named plaintiffs and class members, the *USAA* Court concluded that all three prongs of the *McMorris* test were met. Because two of the named plaintiffs' information had had attempted fraud, there was an objective likelihood plaintiffs' data had been exposed and that at least some portion of the dataset had already been misused. And because the information was systematically targeted by criminals who used sophisticated tools to seek out information about plaintiffs and the class that could then be used to get *additional* sensitive information like driver's license numbers, the information was sufficiently sensitive to support a claim that the plaintiffs had a high risk of identity theft or fraud. Ex. 1 at 4. Those same conclusions are entirely consistent with Ninth Circuit analysis in *Zappos* and *Krottner* and warrant a finding of Article III standing here.[3]

The *USAA* Order also concluded that the plaintiffs there had an independent basis for standing based on allegations of violation of the Driver's Privacy Protection Act ("DPPA"), 18 U.S.C. § 2724. Ex. 1 at 3-4. This analysis is helpful for this Court in analyzing the same claim made by Plaintiff in responding to Defendants' motion to dismiss. *See* ECF No. 33 at

[3] Defendants reiterate their arguments about nonbinding district court decisions that are themselves the subject of previous motions to consider supplemental authority. Plaintiff has addressed these in previous briefs and will not reiterate these arguments here.

14-15. First, Plaintiff does plead a lack of privacy. Compl. ¶¶ 57, 103, Prayer for Relief (d).[4] Second, Plaintiff pleads violation of a privacy-related statute, which is sufficient under the standards articulated in *TransUnion LLC v. Ramirez*, 141 S.Ct. 2190, 2204 (2021). *See* Compl. ¶¶ 84–88.

As the *USAA* Order concludes, and consistent with Ninth Circuit precedent, when "plaintiffs plausibly allege USAA automatically discloses any individual's driver's license information to any third party with 'minimal information' regarding that individual, and, in this instance, disclosed plaintiffs' driver's license numbers to cybercriminals for use in further identity fraud, which plaintiffs plausibly contend would be highly offensive to a reasonable person," that is sufficient to confer standing under the DPPA. Ex. 1 at 4; *accord Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1112 (9th Cir. 2020); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 596 (9th Cir. 2020); *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1274 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937 (2020); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 981 (9th Cir. 2017); *Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1043 (9th Cir. 2017); *Robins v. Spokeo, Inc.*, 867 F.3d 1108, 1117 (9th Cir. 2017); *see also Stasi v. Inmediata Health Group Corp.*, 501 F.3d 898, 909 (S.D. Ca. 2020).

II. THE *USAA* ORDER PROVIDES USEFUL GUIDANCE ON PLAINTIFF'S DPPA CLAIM

In the *USAA* Order, the district court concluded that plaintiffs had plausibly pleaded a violation of the DPPA sufficient to survive a motion to dismiss. Ex. 1 at 5. This ruling is helpful here because it involves a nearly-identical factual scenario as that pleaded in the Complaint. The Court in *USAA* concluded that the plaintiffs' DPPA claim could proceed based on two different conclusions about allegations of a knowing disclosure. First, the Court concluded that the "voluntary decision to automatically pre-fill its quote forms with driver's

[4] If the Court concludes that Plaintiff has a pleading deficiency regarding invocation of a privacy-related interest, Plaintiff respectfully requests leave to replead rather than dismissal.

license numbers constitutes a 'knowing disclosure' of personal information." Ex. 1 at 5 (citing 18 U.S.C. § 2724(a)). Second, the Court concluded that "plaintiffs adequately allege that in light of the two separate data-security alerts that warned USAA as to the vulnerability of its pre-fill data features, USAA reasonably should have known its pre-filling of driver's license numbers would disclose that protected information directly to cybercriminals for impermissible purposes." Ex. 1 at 5 (citing *Gordon v. Softech Int'l, Inc.*, 726 F.3d 42, 54 (2d Cir. 2013); *see also Senne v. Village of Palatine*, 695 F.3d 597, 603 (7th Cir. 2012). The cases that Defendants reiterate from their motion to dismiss have been answered there. *See* ECF No. 33 at 16-18.

Plaintiff also pleads that the disclosure of the information was not for a permissible purpose, and nothing from the *USAA* Order or Defendants' arguments contradict that. *See* ECF No. 33 at 19-21. Defendants "reasonably should have known its pre-filling of driver's license numbers would disclose that protected information directly to cybercriminals for impermissible purposes" and Defendants actively chose to auto-fill information without following the mandates of the DPPA in order to increase its sales volume, which is not a permissible purpose under the DPPA. *See Gordon*, 726 F.3d at 49 ("The default rule is one of non-disclosure."); *Senne*, 695 F.3d at 606.

III. THE *USAA* ORDER PROVIDES HELPFUL NEGLIGENCE ANALYSIS

Finally, the *USAA* Order's analysis of negligence under New York law provides a useful roadmap for allowing Plaintiff's negligence claims to proceed. *See* Ex. 1 at 6-8. In countering this authority, Defendant merely restates arguments previously made in the motion to dismiss; Plaintiff has already answered them and directs the Court to that briefing. *See* ECF No. 33 at 21-23.

CONCLUSION

For the foregoing reasons, Plaintiff respectfully requests leave to file the *USAA* Order as supplemental authority opposing Defendants' Motion to Dismiss (ECF No. 33). The *USAA* Order—which analyzes very similar facts regarding the same security incident involving the

same forms of personal information, and involves plaintiffs similarly experiencing financial fraud in the wake of disclosure of their driver's license numbers—speaks directly to several core questions raised by Defendants in their motion to dismiss, concluding that plaintiffs have standing and their claims should not be dismissed. As a result, good cause exists to allow its filing.

Dated: September 7, 2022

/s/ Michael Kind
Michael Kind
Mk@kindlaw.com
KIND LAW FIRM
8860 S. Maryland Parkway, Suite 106
Las Vegas, NV 89123
Telephone: (702) 337-2322
Facsimile: (702) 329-5881

Gayle M. Blatt (*pro hac vice*)
gmb@cglaw.com
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232

/s/ Kate M. Baxter-Kauf
Kate M. Baxter-Kauf (*pro hac vice*)
kmbaxter-kauf@locklaw.com
Karen Hanson Riebel (*pro hac vice*)
khriebel@locklaw.com
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
Attorneys for Plaintiff and the putative Class